RECEIVED
CENTRAL FAX CENTER

DEC 0 4 2007

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A computer system, comprising:

a chipset;

an internal component of the computer system;

a bus coupled to the chipset to communicate a trusted data cycle to [[an]] the internal component of the computer system; [[and]]

a docking connector; and

a secured docking circuit coupled to the bus and coupled between the bus and a docking connector to scan for the trusted data cycle, detect the trusted data cycle, and provide a filtering mechanism to prevent the trusted data cycle from being provided to a device external to the computer system through the docking connector ~~a device external to the computer system from accessing the trusted data cycle~~.

2. (Original) The computer system of claim 1, wherein the bus is a Low Pin Count bus.

3. (Original) The computer system of claim 1, wherein the component provides protected memory storage.

4. (Original) The computer system of claim 1, wherein the component provides platform authentication.

5. (Original) The computer system of claim 1, wherein the component maintains a protected path between the chipset and a keyboard.

6. (Original) The computer system of claim 1, wherein the computer system is a notebook computer.

7. (Currently Amended) A circuit, comprising:

means for transmitting data on a Low Pin Count (LPC) bus; and

filtering means for scanning for trusted data cycles on the Low Pin Count (LPC) bus and preventing the trusted data cycles on the Low Pin Count (LPC) bus from being accessed by an unauthorized component coupled to a docking connector, wherein the filtering means is coupled between the Low Pin Count (LPC) bus and the docking connector.

8. (Cancelled)

9. (Original) The circuit of claim 7, further comprising:

means for monitoring data cycles on the LPC bus.

10. (Currently Amended) A method, comprising:

monitoring a chipset of a computer system for communication of trusted data cycles on a bus with a secured docking logic;

detecting each of the trusted data cycles by detecting a predefined trusted data cycle indicator with the secured docking logic; and

preventing the trusted data cycles from being available to a component external to the computer system with the secured docking logic.

11. (Original) The method of claim 10, wherein trusted data cycles begin with a "0101" value.

12. (Currently Amended) The method of claim 10, further comprising:

communicating trusted data cycles between the chipset and a first component that provides cryptographic capabilities.

13. (Original) The method of claim 12, wherein the communication between the chipset and the first component is in plaintext format.

14. (Currently Amended) The method of claim 10, further comprising:

communicating trusted data cycles between the chipset and a second component that provides trusted input capabilities.

15. (Original) The method of claim 14, wherein the communication between the chipset and the second component is in plaintext format.

16. (Original) The method of claim 15, wherein the second component maintains a protected path between the chipset and a keyboard, wherein keystroke data is communicated by the chipset to protected memory and trusted applications.

17. (Original) The method of claim 15, wherein the second component maintains a protected path between the chipset and a mouse, wherein pointer data from the mouse is communicated by the chipset to protected memory and trusted applications.

18. (Original) The method of claim 12, wherein the first component protects secret data of the computer system by encrypting the secret data.

19. (Original) The method of claim 18, wherein the secret data is decrypted by hardware of the computer system.

20. (Currently Amended) The method of claim 18, wherein the first component merges data with configuration values of the computer system ~~the computer system's configuration values~~.

21. (Original) The method of claim 18, wherein the first component requests for a system identification request.

22. (Currently Amended) The method of claim 21, wherein a trusted third party chip verifies an identification of the computer system ~~the computer system's identification~~ and sends a response to the first component.

23. (Previously Presented) The computer system of claim 1, wherein the circuit makes a data cycle that is not a trusted data cycle available to the device external to the computer system.

24. (Previously Presented) The computer system of claim 1, wherein if the circuit determines that a data cycle is not a trusted data cycle the circuit does not prevent the device external to the computer system from accessing the data cycle.

25. (Currently Amended) The computer system of claim 1, wherein the circuit blocks the trusted data cycle from [[a]] the docking connector.

26. (Previously Presented) The computer system of claim 1, wherein the trusted data cycle begins with a predefined trusted data cycle indicator.

27. (Previously Presented) The method of claim 10, wherein preventing comprises filtering to block the trusted data cycles without blocking data cycles that are not trusted data cycles.